Common Policy CP Change Proposal Number: 2010-05

To:	**Federal PKI Policy Authority**
From:	Certificate Policy Working Group
Subject:	Proposed modifications to the U. S. Federal PKI Common Policy Framework Certificate Policy
Date:	August 5, 2010
Title:	Changes to Common Policy CP to clarify the archive definition, and how its records are intended to be used.

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy for the U. S. Federal PKI Common Policy Framework Version 3647 – 1.10, April 8, 2010.

Change Advocate's Contact Information:

Name: Cheryl Jenkins
Organization: GSA – FPKI MA
Telephone number: 202-577-1441
E-mail address: Cheryl.Jenkins@gsa.gov

Organization requesting change: Federal PKI Management Authority

Change summary: Clarify the purpose of archiving, and the archiving requirements for auditable events. Also, clarify that NARA and/or other applicable regulations apply. In addition, this change proposal will bring the archive requirements in the Common Policy CP into alignment with the archive requirements in the FBCA CP thereby maximizing the operational efficiency of the FPKI.

Background: In 2008, the FPKIPA adopted a change to the FBCA CP to clarify the purpose of archives records and to list the specific data required to be archived. The FPKI MA would like to maximize the operational efficiency of the FPKI by aligning the archive requirements of the different CAs it manages by bringing the archive requirements in the Common Policy CP into alignment with the FBCA CP archive requirements.

Specific Changes: There are three specific changes listed below.
Text with ~~strikethrough~~ will be removed. Underlined text will be added.

1.) Remove last sentence of the first paragraph in section **5.4, *Audit Logging Procedures***, which requires all audit records to be archived.

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. ~~The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2 *Retention Period for Archive*.~~

2.) Add text indicating that the requirements of NARA and/or other regulatory bodies must be followed. This text will be added to the beginning of section **5.5, *RECORDS ARCHIVE***.

The Common Policy CA must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable.

3.) Modify the list in Section **5.5.1, *Types of Events Archived***, to add audit events that should be archived and clarify audit reporting requirements.

CA archive records will be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data will be recorded for archive:

- CA accreditation (if applicable)
- Certificate policy
- Certification practice statement
- Contractual obligations
- and other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of re-key
- ~~Security audit data (in accordance with section 5.4.1)~~
- Revocation requests
- Subscriber identity authentication data as per section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- ~~Documentation required by compliance auditors~~
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g., audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)

- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

Estimated Cost:
There is no financial cost associated with implementing this change.

Risk/Impact:

None. Positive impact is that archive practices for the Common Policy CA will be brought into alignment with the archive practices of the Federal Bridge CA, making management of the FPKI CAs more efficient.

Implementation Date:

This change will be implemented immediately upon approval by the FPKIPA and incorporation into the Federal Common Policy Framework Certificate Policy.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: TBD
Date presented to FPKIPA: TBD
Date of approval by FPKIPA: TBD